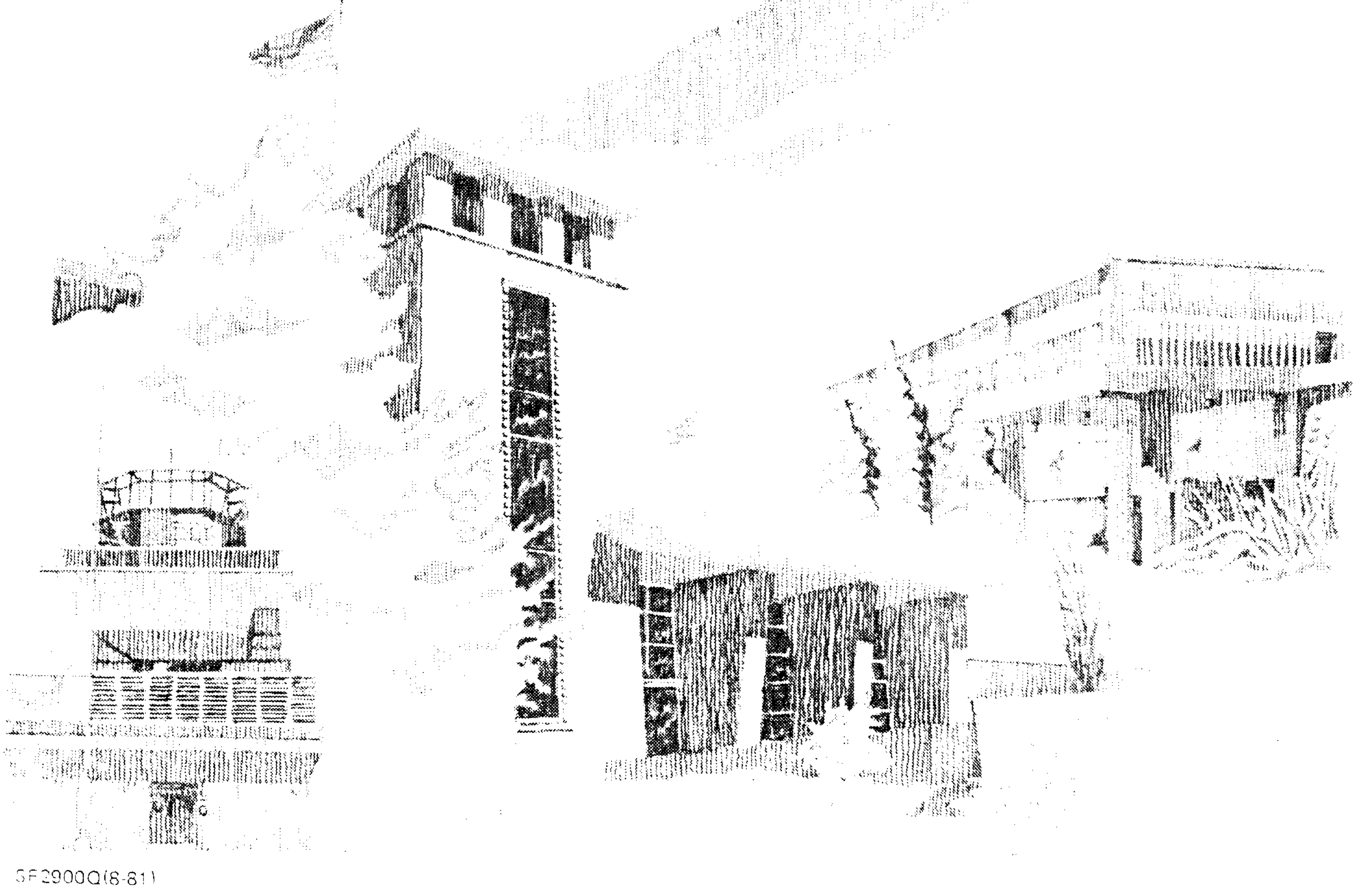
SANDIA REPORT

SAND91–0276 • UC–906
Unlimited Release
Printed June 1991

A Performance Evaluation of Biometric Identification Devices

James P. Holmes, Larry J. Wright, Russell L. Maxwell

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A03
Microfiche copy: A01

SAND91–0276
Unlimited Release
Printed June 1991

Distribution
Category UC–906

A Performance Evaluation of Biometric Identification Devices

James P. Holmes and Larry J. Wright
Facility Systems Engineering Division

Russell L. Maxwell
Systems Engineering Division
Sandia National Laboratories
Albuquerque, NM 87185

Abstract

When an individual requests access to a restricted area, his identity must be verified. This identity verification process has traditionally been performed manually by a person responsible for maintaining the security of the restricted area. In the last few years, biometric identification devices have been built that automatically perform this identity verification. A biometric identification device automatically verifies a person's identity from measuring a physical feature or repeatable action of the individual. A reference measurement of the biometric is obtained when the individual is enrolled on the device. Subsequent verifications are made by comparing the submitted biometric feature against the reference sample. Sandia National Laboratories has been evaluating the relative performance of several biometric identification devices by using volunteer test subjects. Sandia testing methods and results are discussed.

Contents

Figures

A Performance Evaluation of Biometric Identification Devices

Introduction

In many applications, the current generation of biometric identification devices offers cost and performance advantages over manual security procedures. Some of these applications are: physical access control at portals, computer access control at terminals, and telephone access control at central switching locations. An installation may have a single, standalone verifier which controls a single access point, or it may have a large networked system which consists of many verifiers, monitored and controlled by one or more central security sites.

Establishing how well a biometric identification device operates should be an important consideration in any security application. Performance data, however, is neither easy to obtain nor to interpret. Because there are no test standards yet to test against, test methods must be well documented. To measure its theoretical performance limit, a verifier could be tested in an ideal environment with robotic simulation of biometric data. The results of such a test would probably differ greatly from its real-world performance. The human element greatly affects the performance of any identity verifier. Environmental factors such as noise, light, electromagnetic radiation, moisture, dust, and temperature could also affect the verifier's performance.

Sandia began its latest verifier test series in November, 1989. Nearly 100 volunteers attempted many verifications on each machine. Environmental conditions were nominal, as the tests were all performed in a laboratory room for the convenience of the test volunteers. The biometric features used by the suppliers of the latest generation of verifiers in the Sandia tests include:

1. Fingerprint by Identix, Inc.[1]
2. Hand geometry by Recognition Systems, Inc.[2]
3. Signature dynamics by Capital Security Systems, Inc. Sign/On Operations.[3] (Formerly Autosig Systems, Inc.)
4. Retinal vascular pattern by EyeDentify, Inc.[4]
5. Voice by Alpha Microsystems, Inc.[5]
6. Voice by International Electronics, Inc.[6] (Formerly ECCO, Inc.)

General Test Description

Statistics have been compiled on false-rejection error rates and false-acceptance error rates for each verifier. The error rates are described as a percentage of occurrence per verification attempt. "Attempt" is used in this report to describe one cycle of an individual using a verifier as proof of being a validly enrolled user (enrollee). Most verifiers allow more than one try per attempt. "Try" describes a single presentation of an individual's biometric sample to the verifier for measurement. "False-rejection" is the rejection of an enrollee who makes an honest attempt to be verified. A false-rejection error is also called a Type I error. "False-acceptance" is the acceptance of an imposter as an enrollee. A false-acceptance error is also called a Type II error. False-acceptance attempts are passive; these are cases where the imposter submits his own natural biometric, rather than a simulated or reproduced biometric of the enrollee whose identity is claimed. To sum up:

false-rejection error = Type I error = rejection of an enrollee
false-acceptance error = Type II error = acceptance of an imposter.

Each verifier in the test is a commercially available unit. Because of the differences in these units and because we needed an equitable basis of comparison, we attempted to modify some of the units. One goal was to have each verifier report a final decision score for every verification try. Although the manufacturers were generally cooperative, it was not possible to achieve all our goals within the time and budget constraints of the testing. The Identix fingerprint verifier did not generate score data at all. The Capital Security signature verifier scores were not directly related to the accept or reject decision because of some additional decision making after the scores were generated. If a biometric testing standard ever becomes a reality, it should include a section on score data generation and reporting.

Software and/or firmware modifications were made by the manufacturer on some units to allow Sandia to collect the desired test data. All verifiers and specified modifications were purchased by Sandia. Where possible, each verifier was set up in accordance with the manufacturer's recommendations. In most cases, a representative from each manufacturer visited the testing laboratory to verify that his device was properly set up. Where problems were pointed out, attempts were made to rectify them. Some attempts were more successful than others within the limits of our test facility resources.

Testing and Training

The verifier tests at Sandia were conducted in an office-like environment; volunteers were Sandia employees and contractors. A single laboratory room contained all of the verifiers. Each volunteer user was enrolled and trained on all verifiers. There were both male and female volunteers and the efforts of both were valuable to this study. However, for the purpose of simplifying the text, we will use the term "his" rather than "his/her."

There is a learning curve for the proper use of a biometric identification device. As a user becomes more familiar with a verifier, his false-rejection rate decreases. This curve differs for individual users and verifiers. This learning effect was minimized for the Sandia testing by training the individuals before the test, by monitoring their performance, and by eliminating the first few weeks of test data in the results. A number of users were reenrolled on verifiers where there was indication of below-average performance. The transactions prior to the reenrollment were not included in the test results. Some manufacturers recommend that the users be reenrolled as many times as necessary to produce the best enrollment scores. We tended to limit reenrollments to known problem cases due to the relatively short duration of our test, and also to give the verifiers more nearly equal treatment. Verifiers on which it is more difficult to enroll would therefore tend to give somewhat less than optimum performance in our test. This effect is less significant for verifiers which modify the stored reference template by averaging in the biometric samples from successful verification attempts. The EyeDentify and the Identix units are the two tested verifiers that do not modify the reference template.

Other known errors were identified for removal by instructing the users to note on a real-time hardcopy printout any transaction where he made a mistake, or was "experimenting" and did not feel that the verification attempt was valid. A similar method was used to identify invalid transactions on the false-acceptance test. Many hours were devoted to identifying and removing invalid transactions from the data files. There is no doubt, however, that a small number of unrecognized errors remain in the data.

The problem of selecting a representative test user group is most vexing when testing biometric identification devices. While the differences in physiological and behavioral properties of humans are the bases for the devices, these same differences can bias test results between test user groups. The best solution to this problem seems to be to use many users and to make numerous attempts. The larger the numbers, the more likely the results will represent true performance values. Relative performance must be measured against absolute performance. A verifier's relative performance within a user group is generally easier to defend than is the absolute performance.

No extraordinary incentives were offered the volunteer users who performed the tests. Treats in the test room were used to tempt users to remain active. A drawing for a free lunch was offered to the regular users. About 80 of the 100 enrolled users remained fairly active in the tests. Work and travel schedules accounted for the loss of some users. Others simply became disinterested.

First Test Series: False-Rejection Testing

- users attempted verification on each machine many times
- test period was three months long
- users were allowed up to three tries per verification attempt.

Second Test Series:
Passive False-Acceptance Testing

- user submitted the personal identification number (PIN) of other users
- user then submitted his own natural biometric
- users were allowed up to three tries per verification attempt.

Data Processing

The first step in the data processing was to remove the invalid transactions that were noted on the printed data logs generated at each verifier. The data files were then processed to remove incomplete records and to convert the data to a common format. The data was sorted into individual user groups. Records from users making less than six transactions were deleted. User data obtained prior to user group reenrollment on a verifier was also deleted.

A verifier can usually be configured to accept up to three "tries" on a verification attempt. A "try" is one cycle of the user presenting his biometric to the verifier for measurement. To simulate verifier performance on one-, two-, and three-try attempt configurations, our users were instructed to try a third time if verification was not successful on the first or second try. Recorded time- of-day information allowed each score to be identified as either a first, second, or third try.

Up to three tries in a five-minute time interval were considered one verification attempt. Additional tries within this interval were ignored. Tries beyond the five-minute interval were considered another verification attempt. At any given threshold value, a score will produce either an accept or a reject. An accept on the first try is counted as an accept for one-, two-, and three-try configurations. An accept on the second try is counted as a reject on a one-try configuration and an accept on a two and three-try configuration. An accept on the third try is counted as a reject on a one and two-try configuration and an accept on a three-try configuration. Three rejects are counted as a reject on all three configurations. To sum up:

	Configuration Test Result		
Verification Action	one-try	two-try	three-try
Accept on first try	accept	accept	accept
Accept on second try	reject	accept	accept
Accept on third try	reject	reject	accept
No accepts with three tries	reject	reject	reject
No accepts with less than three tries	only actual rejects counted		

The false-reject error rate is the ratio of false-rejects to total attempts at verification. A false reject will be represented as "FR" and is reported in this document as a percentage value. Where transaction score data was available, the FR was calculated for each user for one-try, two-try, and three-try verifier configurations over a range of possible thresholds. The scores were used to find the number of errors that would have occurred had the verifier test threshold been set at each of the possible thresholds.

The false-accept error-rate is the ratio of false-acceptances to total imposter attempts. It will be represented as "FA" and was calculated for each user over the range of possible thresholds and presented as a percentage value.

The FR and FA for each verifier was calculated by averaging the user-percent error rates at each threshold value selected. The FA and FR error-rate curves are shown in the next section, entitled "Results of the Testing." Where possible, error-rate curves are shown for one-try, two-try, and three-try verification attempts. These curves exhibit two general characteristics. One characteristic is the non-zero value of the crossover point of the FA and FR curves. A second characteristic is the trend toward a lower rejection rate as the number of tries at verification increases. Both these characteristics force some tradeoffs in using these verifiers.

The non-zero error value at the crossover point means that there is no threshold setting where both the FA and FR error-rates are zero. The user must choose a threshold setting to fit the application. As the threshold is moved toward tighter security (higher rejection error rates), both imposters and valid users face higher rejection rates. Both are rejected less often when the threshold is moved toward lower security. The point at which the FA and FR curves cross over is referred to as the equal-error setting. This single-value error rate has been accepted as a convenient value to describe the performance of a verifier in the Federal Information Processing Standards Publication (FIPS PUB) 83. This and other single-value criteria have been used to characterize verifier performance, but no single value can provide much insight into the true performance capability of any verifier. The FA and FR error-rate curves provide much more insight into performance and should be examined for suitability in any security application.

Multiple-try attempts at verification can improve the performance of some biometric verifiers. The rejection rate for valid users generally decreases faster than the rejection rate for imposters, as more verification tries are allowed. Valid users are generally rejected because of inconsistent presentations of their biometric input. Additional tries allow the valid user to correct the inconsistencies and to generate an acceptable input that matches the reference template. Imposters are generally rejected because their biometric is not close enough to the reference to be accepted. Additional tries increase the chances of imposter acceptance if the biometric differences are small enough to be masked by the inconsistent user inputs and by tolerant threshold settings.

The Identix fingerprint verifier we tested did not have a customer adjustable system threshold. While individual thresholds could be adjusted, we did not get any test data at other than the factory-set threshold. The other verifiers tested did provide test score data, but the Capital Security signature verifier scores could not be used to generate error-rate curves because of a second calculation that it uses to make the accept or reject decision.

Our transaction time results were obtained by timing the users from when they touched the verifier until the verification attempt verdict was given. The users were not told that they were being timed. We feel that the results reflect verification times that would be typical in an actual installation. These times are substantially longer than the minimum times of a skilled user in a hurry.

Results of the Testing

Alpha Microsystems Results

Alpha Microsystems of Santa Ana, California bought out Voxtron and is now selling an updated system called Ver-A-Tel. This voice verification system makes use of a personal computer (PC), which contains the speech board hardware and the software programs. User terminals are touch-tone telephones. The Ver-A-Tel system is offered in two similar versions: the telephone intercept system (TIS) and the remote-access system (RACS). We tested the public TIS version, but not the direct-line RACS version.

The software supplied with the system provides the necessary management functions to enroll and delete users, to configure the system parameters, to display activities and alarms and to generate reports. Because this password-protected software is menu driven, it allows the security manager to select options from the screen and to fill in the blanks to configure the system. A supplied user's guide provides any additional information that might be needed.

Users were enrolled on the same touch-tone telephone that was later used to access the system. Prior

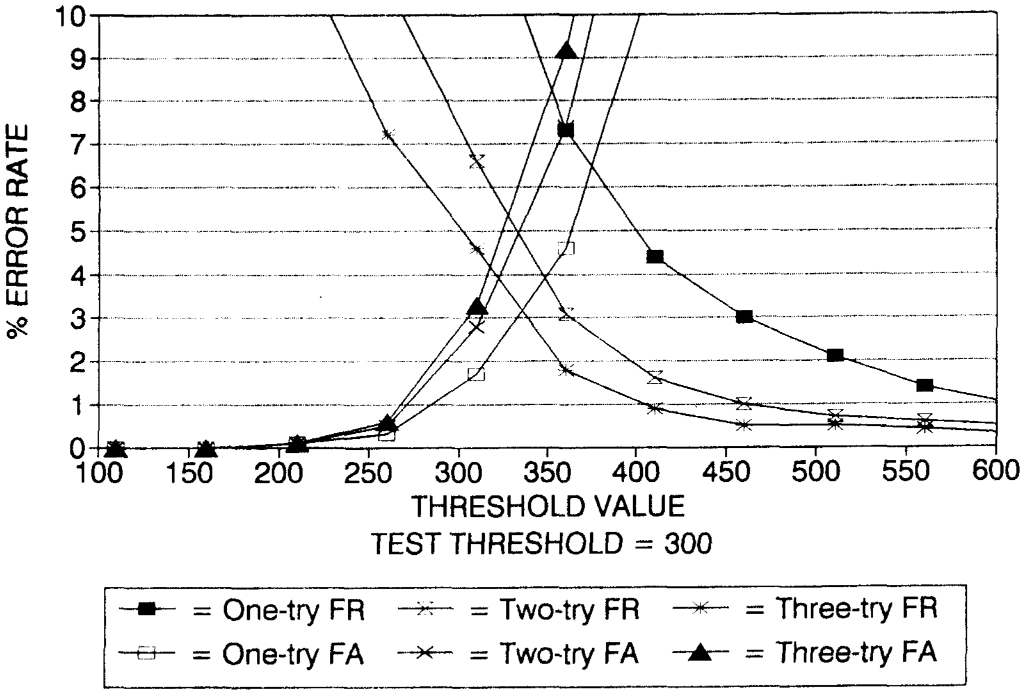


Figure 1. Alpha Microsystems Voice Verifer

Capital Security Systems, Inc. Results

Capital Security Systems, Inc. of Columbia, MD purchased the signature dynamics verifier line from Autosig Systems, Inc. This verifier consists of a user interface tablet and a controller which is designed to integrate into a host-computer access control system. The Capital security system offers products for both physical entry control and data access control. The user interface is similar for both applications. A variety of hardware and software options allow the system to function in applications from stand-alone protection of a single entrance to networked, host-based systems.

The user interface is a desk top tablet (~9 3/8 by 11 inches) that incorporates a digitizer tablet, a magnetic stripe card reader, and a tethered pen. The digitizer tablet (~2 1/2 by 5 inches) is the area where the user actually signs his name with the tethered pen. The system measures the dynamics of the user's signature to form the biometric template for enrollment and verification.

The controller can function as a stand-alone device with the user interface and door interface hardware, but must be connected to a computer for programming and user enrollment. An IBM PC or a higher class, compatible computer with a serial port and a floppy disk drive can be used. The computer class must match the controller interface requirement.

Software is provided to allow the security manager to configure the system and to enroll users. A menu-driven program provides the manager with the necessary options. Before a user can be enrolled, a user data record must be generated in the user data file. The manager selects the options and fills in the blanks to generate the record. For the model tested, a magnetic stripe card was required for ID entry. It was coded with the user's PIN and provided to the user for verifiers in this test series.

To enroll, the user must follow the illuminated prompts on the interface tablet. First the user PIN is entered with a swipe of his magnetic stripe card through the card reader. Next, the user is prompted to alternately sign on and wait while the system generates a template. Finally, the user is prompted when the sequence is complete. It normally takes two signatures and one verification signature to enroll. The signature must be within the marked digitizer pad area, using the tethered pen. The system can be used with a regular ball-point pen tip and a stick-on paper sheet over the pad, or with an inert, inkless pen tip system directly on the digitizer pad.

Verification is similar to enrollment. The user PIN is entered with the magnetic card and the user signs his name on the digitizer pad with the tethered to enrollment, the security manager created a record for each user and each was assigned a unique PIN. An optional secret enrollment passcode, to prevent an imposter from enrolling in place of the authorized user, was not tested.

A phrase is required for enrollment and subsequent verification. The security manager can select from a number of standard phrases on the menu display; from this selection, he can allow the user to make up his own phrase. There are some restrictions on user-selected phrases, such as the minimum and maximum length and the optimum number of syllables. These options are discusssed in the User's Guide which is supplied with the system.

Voice verifier manufacturers are quick to point out that security is enhanced if each user has a secret phrase. These manufacturers, however, do not address the problem of how to keep a phrase secret that must be uttered into a microphone. On the other hand, it is certainly less likely that an imposter would be accepted if he does not know the proper phrase. It is even plausible that a valid user could have a lower false-reject error rate with a chosen phrase that was more natural or familiar to him. The objective of our test was to measure the ability of the system to verify users based solely on their biometric properties. Thus, we assigned the same phrase to all users.

To enroll, a user calls the verifier telephone number. The system answers and instructs the user to enter his PIN on the touch-tone keypad. If the system finds that the PIN belongs to someone who is not yet enrolled, it tells the user what he must do to enroll. This may include an instruction to enter the proper enrollment passcode on the keypad. The user is instructed to say the verification phrase a number of times. The system performs checks on each response and may prompt the user to be more consistent and to repeat the phrase again. When the system parameters for a successful enrollment are met, the system so informs the user. A user template is generated from the enrollment data and is stored for future verification of the user's identity. The system may tell the user that the enrollment was better than most. This indicates that the enrollment phrases were very consistent. It is also possible for the user to fail. In this case, the user is told to practice and try again. The security manager can also check the enrollment scores to get a measure of the enrollment performance. Individual accept or reject thresholds can be set by the security manager to compensate for differences in user performance. This adjustment is made (plus or minus) to the system threshold setting.

On verification attempts, an enrolled user's PIN is recognized by the system and is used to retrieve the proper template from the enrollment database for verification. The user is then prompted to say the phrase for verification. Optionally, the new phrase data may be averaged into the stored template to update the template each time the verification is successful. In time, if the user becomes more consistent and the verification scores improve, the security manager may opt to adjust the user threshold value to a more secure value. Experienced users generally skip the voice prompts because a preceding tone signals the user that he can go ahead without further delay if he does not need the voice instruction.

The time information given for the Alpha Microsystems voice verifier is different from other verifiers because it includes dialing a 5-digit telephone number and waiting for the verifier to answer. We included this scenario because the telephone access method was also used in our test verifier. Other access methods may result in different transaction times. The minimum time of ~13 seconds was necessary to perform the following steps:

- lift the phone and dial a 5-digit extension
- wait for the voice system to answer and generate the tone prompts (without waiting for the subsequent voice prompts)
- enter a 4-digit PIN on the phone keypad
- say "yankee doodle dandy"
- be verified.

The average user in our test took ~19.5 seconds for a complete verification. This average includes multiple-try attempts when this was required by the system.

The crossover point where the one-try false-reject and the one-try false-accept curves are equal has an error rate of 6.5% at a threshold value of ~375. At the test threshold setting of 300, the three-try, false-reject error rate was 5.1% and the three-try, false-accept error rate was 2.8%.

There were 5434 transactions in the false-reject test and 2990 transactions in the false-accept test. The results of these tests are shown in Figure 1.

pen. A prompt then tells the user whether the verification was successful or if another signature try is necessary. Two tries are usually allowed. Each successful verification is averaged into the reference template to allow the system to accommodate long-term changes in the user signature. This averaging can be inhibited by the security manager.

Imposter testing consisted of each imposter entering PINs by using the magnetic stripe badges of all other users. The imposter knew the real user's name from the badge, but did not have a sample of the user's signature. The imposter was free to try to sign the actual user's name. As a matter of interest, we attempted some verifications by tracing over valid signatures. The scores were generally much worse than other imposter attempts because of the importance of the signature dynamics in verification. None of the tracing attempts were included in our test results.

The time to perform a verification depends in part on how long a user takes to sign his name. Our users averaged ~15 seconds to verify on the Capital Security system; this time includes PIN entry via a swipe card reader and some multiple-try attempts as required by the system. The minimum time observed was ~12 seconds.

Error-rate curves are not shown because the Capital Security accept or reject decision process is more than just a function of the transaction score. A second decision calculation is performed on all tries that produce a score between 16,000 and the verifier threshold setting. The threshold was set at 21,000 for our test.

All false-accept and false-reject error rates obtained were from a count of the errors at the operational threshold:

False-Reject Error Rate	Percentage
three-try	2.06%
two-try	2.10%
one-try	9.10%

False-Accept Error Rate	Percentage
three-try	0.70%
two-try	0.58%
one-try	0.43%

The Capital Security is usually set up for two tries.

There were 3106 transactions in the false-reject test and 6727 transactions in the false-accept test. The Capital Security system error-rates are shown in Figure 2.

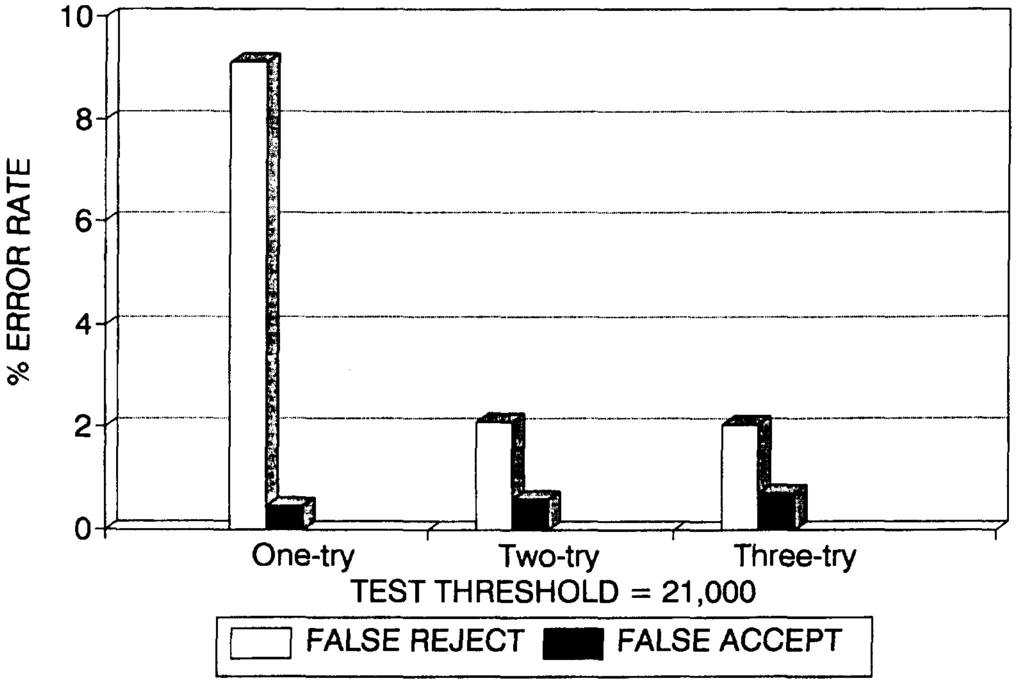


Figure 2. Capital Security Signature Dynamics

International Electronics (ECCO VoiceKey) Results

International Electronics, Inc. of Needham Heights, MA purchased ECCO Industries, Inc. of Danvers, MA and now markets the ECCO VoiceKey. The VoiceKey is a self-contained, wall-mounted user interface that communicates with a controller over a copper wire cable. The user interface contains an alphanumeric display, keypad, a microphone, an audible beeper, and indicator lights. Keys, displays, etc. allow all necessary functions to be performed at the user interface. Some of these functions are user enrollment and system management.

The user interface and controller can operate in a stand-alone mode to provide security at a single entry point, or can be networked through a network controller to other units in a security system. A VoiceKey network has a master voice reader and slave voice readers. The master voice reader is normally used for all enrollments and programming, which are then downloaded to the slave readers. Enrollment and programming can be performed at any slave, but it cannot be downloaded to any other reader. A printing capability allows audit information to be output to a printer connected to the controller of the master reader.

User enrollment is normally performed at the master voice reader by a security manager who is authorized to enter the programming mode. This authorization must be verified by voice before the programming mode can be entered. Programming is accomplished by keypad key inputs. Message displays and lights provide feedback to the programmer as the program steps are entered. A supplied programming manual provides complete information on the programming procedures. A user program allows new users to be added. This option requires the security manager to enter a unique PIN to access zone data and to enter the user authorization level for the new user. The reader then displays a series of message and colored-light prompts for the new user to initiate the sequence and to say his password several times. A red/green light display at the end of the enrollment sequence informs the new user of failure/success in enrolling. (This frustrates color-blind users who cannot distinguish between the red and green colors.) If successful, the new user can practice using his password as desired. Each successful verification causes the user's template to be modified by the new input.

Verification can be accomplished in ~5 seconds. Users averaged ~6.6 seconds per one-try attempt; in this time, they were able to enter a 4-digit PIN on the keypad and to utter the single password.

The crossover point where the one-try, false-reject curve and the one-try, false-accept curve are equal has an error-rate of 8.2% at a threshold value of 100. Only one-try, false-accept data was obtained for the VoiceKey verifier. There are three user thresholds available for the VoiceKey verifier. Security level 1 is a threshold of 75, level 2 is a threshold of 65 and level 3 is a threshold of 55. At the test threshold setting of 75, the three-try, false-reject error rate is ~4.3%, and the one-try false-accept error-rate is ~0.9%.

Voice verifier manufacturers are quick to point out that security is enhanced if each user has a secret phrase. These manufacturers, however, do not address the problem of how to keep a phrase secret that must be uttered into a microphone. On the other hand, it is certainly less likely that an imposter would be accepted if he does not know the proper phrase. It is even plausible that a valid user could have a lower false-reject error rate with a chosen phrase that was more natural or familiar to him. The objective of our test was to measure the ability of the system to verify users based solely on their biometric properties. Thus, we assigned the same phrase to all users.

We experienced high, false-rejection error rates with the assigned password. The manufacturer's representative suggested that each user be allowed to choose a password familiar or comfortable to him. We gave additional training and reenrolled ~15% of the users that were experiencing the most trouble with verification. On reenrollment, the users could choose from several suggested words. Some were allowed to select a word of their choice. This effort did produce better verification scores for many of the individuals after they were reenrolled. We were unable to correlate the effect of reenrollment on the long-term, false-rejection error rates. Several variables remain in the verification process. As the user becomes more familiar with a password, he would be expected to get more consistent in its use. The user's reference template is also modified for each successful verification, and thus should improve the verification scores of consistent users. An analysis of entire user group performance before and after reenrollment, however, did not show a significant improvement over time.

There were 4871 transactions in the false-reject test and 3270 transactions in the false-accept test. The graphical results of these tests are shown in Figure 3.

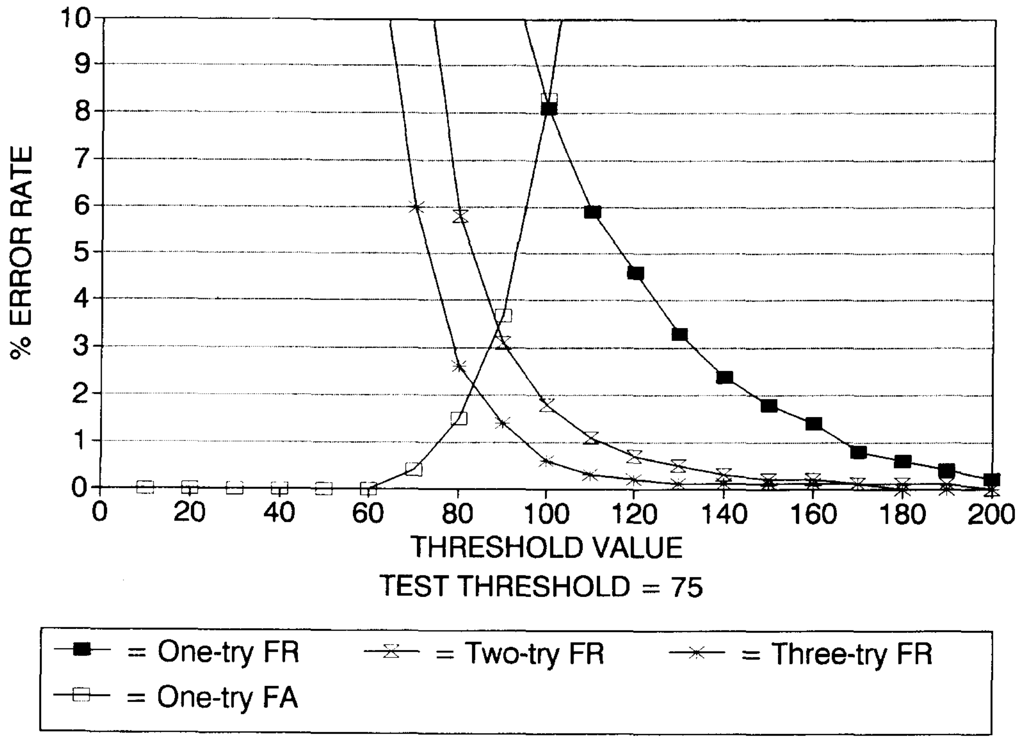


Figure 3. International Electronics Voice Verifier

EyeDentify Verify Mode Results

The retinal pattern verifier in this test series was Model 8.5, manufactured by EyeDentify, Inc. of Portland, Oregon. The verifier includes a reader and a controller. The reader contains an aperture where the user looks to align his eye with an optical target, which appears as a series of circles. As the user moves his eye around, the circles become more or less concentric. Proper alignment is achieved when the circles appear concentric and the user is looking at the center of the circles. The reader also contains a display, a keypad, and an insertion reader for magnetic stripe cards. A copper cable connects the reader to a controller box that contains processing and interface electronics.

The controller can function as a stand-alone device with the user interface and door interface hardware, but must be connected to a computer for programming and user enrollment.

Two readers were tested. Reader 1 was set up to operate in the verify mode using a PIN entered via an insertion card. Reader 2 was set up to operate in the "hands-free" recognize mode. The results for Reader 1 are discussed in this section, and the results for Reader 2 are discussed in the following section entitled: "EyeDentify Recognize Mode Results."

The software allows the security manager to configure the system and to enroll users. A menu-driven program provides the manager with necessary options. Before a user can be enrolled, a user data record must be generated in the user data file. The manager selects the options and fills in the blanks to generate the record. Once the record generation in the enrollment sequence is completed, a message instructs the user to enroll. The new user then aligns the optical target in the viewing aperture and presses the "ENTER" key on the keypad to initiate the eye-scan sequence. Each subsequent scan generates a score on the computer display and allows the security manager to accept or reject it. The user template is generated from an average of the accepted scans on enrollment. This template is not modified by subsequent verifications, so it is important to take some care during enrollment and not to accept scores below the mid 70s. It is not difficult for most properly instructed users to score above 80.

The user's PIN must be entered for verification. The EyeDentify 8.5 allows either manual entry on the keypad or automatic entry by using the card reader. Our tests used the card entry option. The average time for our users to perform the verification process was ~7 seconds. This time included some multiple-try attempts and the removal of glasses by some users after inserting their card. The quickest times were around 4.5 seconds.

The false-reject error rates for EyeDentify Model 8.5 in this test are significantly less than for the Model 7.5 we tested in 1987. There are two differences between the models we tested that could account for the decrease in these errors:

1. Improved data acquisition software for Model 8.5 now tests for eye fixation before accepting a scan. This feature reduces the chance of a rejection due to eye movement.
2. The Model 7.5 we tested used only keypad PIN entry, while the Model 8.5 we tested used magnetic card PIN entry.

The verify mode crossover point, where the one-try, false-reject error rate and one-try, false-accept error rate are equal, was ~1.5% at a threshold of ~45 for Model 8.5. At the test threshold setting of 70, the three-try, false-reject error rate was 0.4%. No false-accepts were recorded at this threshold value. There were 5134 transactions in the false-reject test and 4196 transactions in the imposter test. The test results for Reader 1 are shown in Figure 4.

EyeDentify Recognize Mode Results

A unique option of the Model 8.5 verifier is the "hands-free" mode of operation. While the verifier is operating in this mode, the user merely peers into the viewing aperture and aligns an optical target by positioning his head. The verifier senses the user's presence, takes a scan, and decides whether or not the scan data is from an eye. If a digital pattern is generated from an eye, the verifier searches the template data base for a match. If a match is found, the verifier recognizes the user as valid. Otherwise, the user is requested to "REPEAT" up to two more tries until a valid match is found. The user is rejected if a match is not found in three tries.

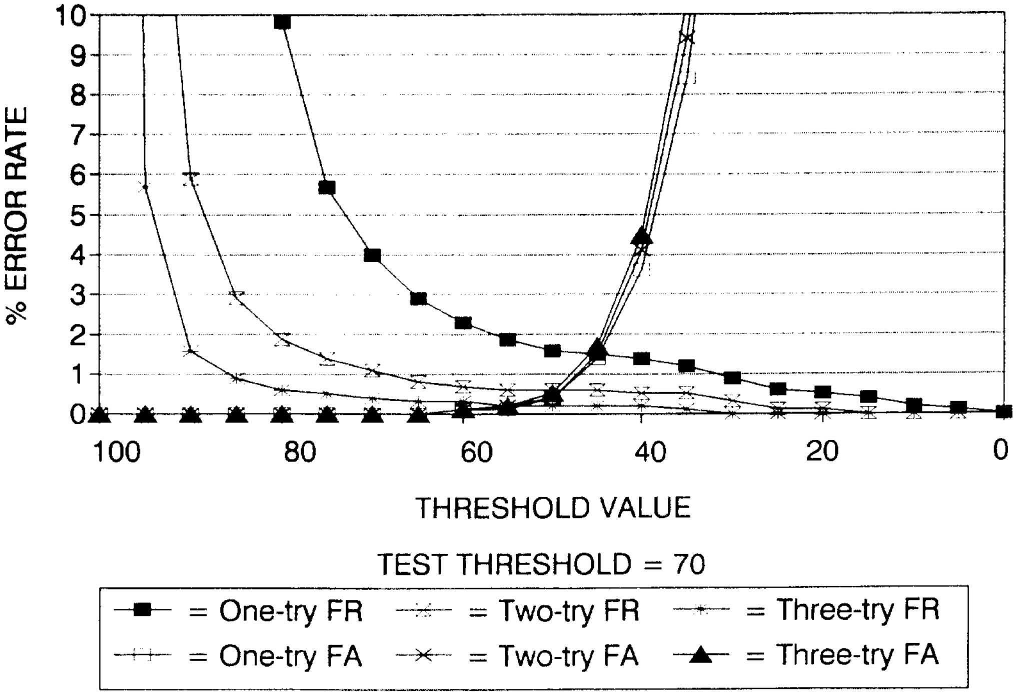


Figure 4. EyeDentify Eye Retinal Pattern

No timing information was taken for the recognize-mode operation because there is no precise point that can be observed when the user initiates the sequence. The user peers into the aperture, aligns the target, and waits for the target to turn off at the end of the scan. The auto-scan feature eliminates the need to insert the magnetic card and press the START button, cutting ~2 to 3 seconds from the verify-mode transaction time. We had a user database of ~100 users that had to be searched to find a matching template for each transaction. This searching did not add a noticeable time delay to the transaction. Larger databases will add more search time to each transaction.

The threshold was set to 75 for the recognize mode of operation. This means that any scan that produces a score of 75 or less is rejected as not being a member of the enrolled user base. A score of greater than 75 causes an accept, and the name of the identified user is displayed on the reader.

There were 5072 transactions recorded on the recognize-mode reader. A transaction is defined as any scan the machine decides meets the minimum criteria to be an eye. None of these scans resulted in a false accept. This result is especially significant because the 100 user database multiplies the possible matches to over half a million!

False-reject information cannot be reported on the "hands-free" recognize reader because there is no PIN associated with a reject that can tie it to a user. No doubt the false-reject rate is significantly higher in the recognize mode because the user does not control the start of the scan. In many attempts, the scan started before the user had the target properly aligned. With practice, most users learned to use the recognize mode to their satisfaction. EyeDentify has now modified their acquisition software to allow users more time to align the target. This change should lower the false-reject error rate.

Identix Results

The fingerprint verifier evaluated in this test was the TouchLock, manufactured by Identix, Inc. in Sunnyvale, California.

The user interface to the Identix system is a sensor module that contains the finger platen/scanner hardware, a display, a keypad and communications electronics. This module is ~8.2 inches wide, 4.4 inches tall, and 3.9 inches deep. The sensor module communicates with a remote processor module over a copper wire cable. The remote module contains the processor, memory, input/output hardware, and communications hardware to support stand-alone operation at a single entry point or in a network environment. Our test verifier was connected to a host computer with the Identix TouchNet software support system. It also was connected to a magnetic-stripe, swipe-card reader via its built-in card reader interface. The card reader was used to enter user PIN information for verification attempts.

The Identix supplied software is a password-protected, menu-driven program for IBM PC and compatibles. It provides the capability to configure the system, to set up user records, and to generate reports.

User enrollment is performed at the sensor module. A security manager must first be verified by a fingerprint scan before the enrollment mode can be entered. Messages on the sensor module display provide user prompts and status information. A unique PIN must be entered for the new user, followed by a number of finger scans that allow the system to generate a template. If the enrollment is successful, a quality rating is displayed. The manager can accept or reject the enrollment at this point. The manufacturer recommends that only "A" or "B" quality ratings be accepted. A "C" rating is the least desirable. If the enrollment is unsuccessful, the system informs the user, who is invited to try again. The templates are not modified by subsequent verifications, so if problems appear, the user should be enrolled again.

We accepted some "C" enrollments for our test. We retrained and reenrolled users that experienced the most problems with verification. The reenrollment did not always result in a higher quality rating. A number of our users appear to have poor quality fingerprints that would not produce good results, even when other fingers were tried. Another problem was caused by low humidity during our test period. User's skin would dry out to the point where the system could not verify the user. Lotion or skin moisturizer often solved the dryness problem.

Our users all had the factory-default verification threshold of 125. The host system software allows the security manager to change individual threshold values, but we did not exercise this option. Our test results do not include the error-rate curves because this verifier did not generate verification score information. Only the percentages of false-reject errors and the false-accept errors at the factory-default threshold can be reported.

The lack of score data hampered our attempts to quantify the Identix verifier. Enrollment quality ratings were generated from groups of finger scans. Individual scan quality was not available. Some clues were available from prompts to position the finger further up or down on the platen, but we could not correlate the finger positioning to scan quality. Our false-rejection error rates were significantly worse than the estimated error rates published in the Identix TouchNet User's Guide, supplied by Identix with the TouchNet system. Identix indicates an estimated single-try, false-rejection error rate of ~3% for an enrollment threshold setting of 125. We experienced over 9% false-rejections for three-try attempts with the 125 threshold setting. The cold, dry weather effect on skin conditions in Albuquerque could account for some of this difference. Individual score data might have given us more insight into the problem.

Our users averaged ~6.6 seconds for a card PIN entry verification, including multiple-try attempts. The fastest users verified in under 5 seconds.

Two identical readers were used in this test. The two readers tested were set up for a maximum three-try attempt and only reported a single accept or reject transaction result for each attempt. If a user was accepted on either the first, second, or third verification try, the attempt was recorded as an accept. If a user was rejected on all three tries, the attempt was recorded as a reject. Individual-try data was not available from the monitoring program.

Reader 1 logged 2248 verification attempts with a false-reject error rate of 9.4% and no false accepts. Reader 2 logged 2316 attempts with a false-reject error rate of 9.5% and no false accepts. The number of false-accept attempts was 3424. The false-reject error rate equals the percentage of the three-try false-rejects that occurred in the verification attempts.

Recognition Systems, Inc. Results

The Model ID3D-U hand-profile verifier manufactured by Recognition Systems, Inc. (RSI) of San Jose, California was evaluated in this test. The verifier houses the hand geometry reader and all the electronics in one enclosure. Both the wall mount or the desk top models are available. The reader has a platen with guide pins to aid in proper hand placement; an optical imaging system acquires the hand geometry data. Displayed messages prompt the user and provide status information. A keypad and an insertion magnetic-stripe card reader record user data input. This verifier can be configured for stand-alone operation or for use with a host processor. Our test verifiers were configured for use with a host processor. The host management software we used included some custom features not required for normal system operation.

User enrollment takes place at the verifier reader. In actual security system applications, each user is assigned an authority level and, if required, a password for entering the security management command mode. A new user can only be enrolled by a security manager with the proper authority level and password to enter the enrollment sequence. The manager must first be verified on the hand geometry reader, and then he must enter the proper password within a time limit to initiate the enrollment sequence. Our test software did not require a password or manager verification for user enrollment. It provided the necessary functions with a menu-driven program that allowed the test conductors to fill in the blanks and to initiate the enrollment sequence.

User Enrollment Sequence

1. A valid PIN is entered by the new user.
2. A ** PLACE HAND ** message then appears on the reader display.
3. The user must then place his hand on the platen and against the guide pins.
4. When the imaging system determines that the hand is properly positioned within the time limit, the hand geometry data is acquired and a ** REMOVE HAND ** message is displayed.
5. The message display prompts are repeated at least two more times, and the user reference template is then generated from an average of the three inputs.

User Verification Sequence

1. Enter the user PIN by keypad or card reader.
2. Follow the ** PLACE HAND ** and ** REMOVE HAND ** instructions on the display.

The average verification time for our users was ~5 seconds, with card PIN entry. (Times as low as ~2.9 seconds were observed.)

The false-reject error rates for Model ID3D-U in this test were less than the rates were in 1987 when we tested the Model ID3D-ST. PIN entry by magnetic card rather than by keypad is the most likely reason for the lower error rates.

The crossover point, where the one-try, false-reject error rate and the one-try, false-accept error rate are equal, was ~0.2% at a threshold of ~100 for Model ID3D-U. At the test threshold value of 75, the three-try, false-reject error rate was less than 0.1% and the one-try, false-accept error rate was ~0.1%. Three-try, false-accept error rate data was not obtained in this test. The test results were very similar on both readers; thus, only Reader 0 results are plotted.

Reader 0 logged 5303 transactions in the false-reject test and 5248 transactions in the imposter test. Reader 1 logged 5285 transactions in the false-reject test and 3839 transactions in the imposter test. The results of this test are shown in Figure 5.

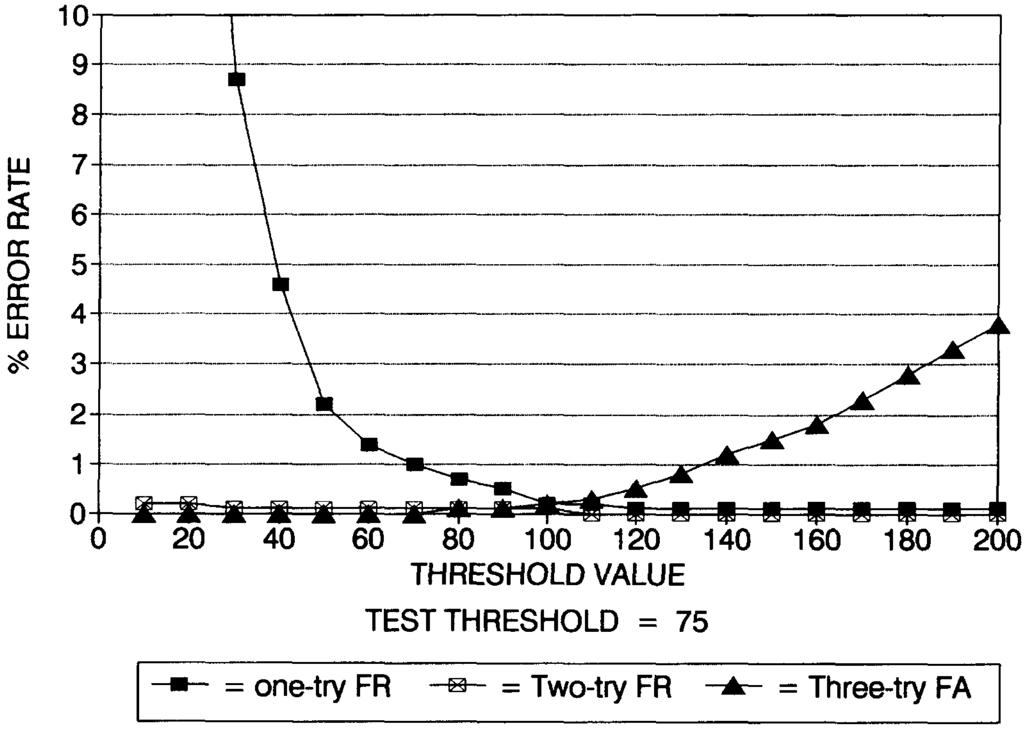


Figure 5. Recognition Systems Hand Geometry

Summary

The relative performance of the tested verifiers can be deduced from the test results. These results include the user variables in the operation of the machines and are therefore representative of the performance that can be expected with average users; at the same time, they are not a true measure of the machines absolute performance limits. The degree to which our results differ from the performance limits is an indication of the complexity of the user interface. As an interface becomes more complex, more user variables are introduced that could shift the test results away from the performance limit.

From a test viewpoint, it is desirable to have a final score value reported for each verification try. This report is not possible, however, because some verifiers do not provide the score data necessary for us to calculate error-rate curves. Verifier results in this case are given only for the one threshold value tested. It would have been possible to repeat the performance tests at a number of different threshold values to obtain points on the error-rate curves, but we did not have the resources for such an extensive test. This is only one of several roadblocks for developing biometric verifier testing standards.

A user survey was taken late in the test. The summary results are given in the appendix. Users generally preferred the verifiers that produced the fewest false-rejects and which took the least time to use. User frustration grew rapidly with high, false-rejection rates; these rates proved to be a bigger problem for them than did the slow transaction times. The RSI hand geometry was overall the user favorite.

The verification timegraph (see Figure 6) shows the average transaction times for:

- entering the PIN
- presenting the biometric feature
- verification or rejection.

The Alpha Microsystems time also includes the time necessary:

- to dial a five-digit number on a touch-tone telephone
- wait for an answer from the system.

This data was obtained by timing the users without their knowledge. These times are representative of actual-use transactions; they are not intended to indicate the minimum times possible.

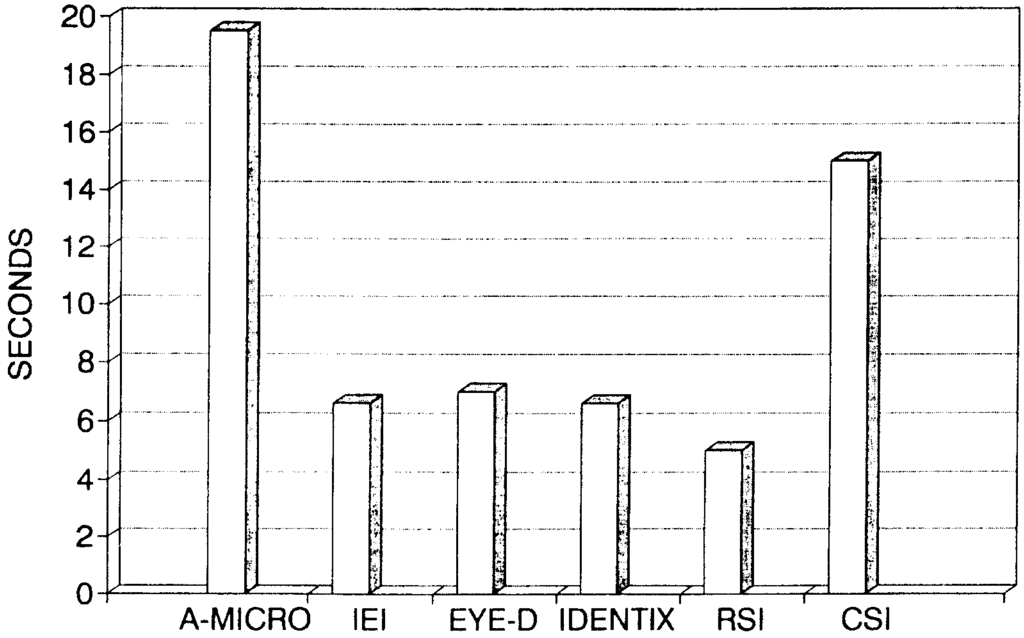


Figure 6. Average Verification Time in Seconds

Conclusions

Performance is a very important issue, but it is not the only factor in choosing a biometric identification device. The device must also be suitable for the facility in which it is installed. The present generation of biometric identification devices provides reliable and cost-effective protection of assets. Available computer interfaces and software provide effective security management with real-time control, transaction logging, and audit-tracking capabilities. The current need in the biometric identification field is to have the market make greater use of what already exists. While new biometric devices are still emerging, it is unlikely that any of them will turn the market around with a price or performance breakthrough.

The error-rate curves contain much more information about the performance of the verifiers than was included in our individual discussions. Manufacturers can provide additional information about how to apply their devices to specific requirements. Finally, it is important to keep the error rates in perspective to the real world. A 3% false accept means that there is a 97% probability that an imposter will be detected.

References

[1] Identix, Inc., 510 N. Pastoria Ave., Sunnyvale, CA 94086, (408) 739-2000

[2] Recognition Systems, Inc., 1589 Provencetown Drive, San Jose, CA 95129, (408) 257-2477

[3] Capital Securities Systems, Inc., Capital Security Operations, 9050 Red Branch Road, Columbia, MD 21045, (301) 730-8250

[4] EyeDentify, Inc., PO Box 3827, Portland, OR 97208, (503) 645-6666

[5] Alpha Microsystems, 3501 Sunflower, Santa Ana, CA 92704, (714) 957-8500

[6] International Electronics, Inc., (ECCO) VoiceKey, 32 Wexford St., PO Box 584, Needham Heights, MA 02194, (617) 449-6646.

APPENDIX

User Survey Results

	ALPHA		EYEDENTIFY			RECOGNITION	AUTOSIG	
Which machine do you feel:	MICRO	ECCO	VERIFY	RECOGNIZE	IDENTIX	SYSTEMS	SIGNON	NONE
1. is the easiest to use?	0	4	2	22	15	35	1	0
2. is the fastest?	1	4	1	28	8	35	0	0
3. is the slowest?	38	5	1	2	9	0	24	1
4. rejects you most often?	11	36	2	5	17	1	6	0
5. rejects you least often?	11	6	10	11	12	42	9	0
6. requires most concentration?	10	25	12	23	6	1	4	0
7. requires most proficiency?	11	23	9	15	11	1	9	4
8. requires least proficiency?	5	6	4	9	12	38	6	1
9. is most frustrating to use?	10	34	2	12	12	0	5	3
10. is most friendly/fun?	5	2	6	17	13	31	6	1
11. gives health/safety concerns?	1	0	23	21	1	5	0	47
12. gives invasion of privacy concerns?	0	1	2	2	3	1	16	56
13. was most difficult to enroll on?	17	21	1	1	15	2	3	18
14. was most intimidating to use?	5	16	4	6	4	0	2	41
15. best to secure a computer terminal?	7	4	12	10	22	18	7	9
16. best for door security?	3	7	18	19	13	27	3	4
17. best for bank/POS use?	1	0	13	8	21	11	23	6
18. best for large population?	2	2	5	14	16	38	3	8
19. Did you like card or pin best?	Card: 56		Pin: 17	None: 3				

NOTES:
1. Number of respondents: 76
2. Respondents were allowed to make multiple responses to each question.

DISTRIBUTION:

1 Edward J. McCallum, Director
Office of Safeguards and Security
US DOE
SA-10
Washington, DC 20545

1 William L. Barker, Acting
Dep. Asst. Secy. for Security Affairs
US DOE
SA-1
Washington, DC 20545

1 David A. Jones, Acting Director
Policy, Standards and Analysis Division
Office of Safeguards and Security
US DOE
SA-12
Washington, DC 20545

1 William J. Desmond, Chief
Physical Security Branch
Office of Safeguards and Security
US DOE
SA-121
Washington, DC 20545

1 Larry D. Wilcher, Chief
Technical and Operations Security Branch
Office of Safeguards and Security
US DOE
SA-123
Washington, DC 20545

1 Jerry C. Howell, Deputy Director
Field Operations Division
Office of Safeguards and Security
US DOE
SA-13
Washington, DC 20545

1 Donald C. Tubbs
Assessment and Integration Branch
Office of Safeguards and Security
US DOE
SA-131
Washington, DC 20545

1 Ernest E. Wagner, Chief
Weapons Safeguards and Security Operations
Branch
Office of Safeguards and Security
US DOE
SA-132
Washington, DC 20545

1 A. J. Heysel, Chief
Production/Energy Safeguards/
Security Operations Branch
Office of Safeguards and Security
US DOE
SA-133
Washington, DC 20545

1 G Dan Smith, Chief
Planning and Technology Development Branch
Office of Safeguards and Security
US DOE
SA-134
Washington, DC 20545

1 Carl A. Pocratsky
US DOE
SA-134
Washington, DC 20545

1 Marshall O. Combs, Deputy Director
Headquarters Operations Division
Office of Safeguards and Security
US DOE
SA-14
Washington, DC 20545

1 David A. Gurule, Acting Director
Security and Nuclear Safeguards Division
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

1 Donald J. Cook, Director
Attn: Stan Laktosic, Tom Golder
Central Training Academy
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

DISTRIBUTION (Continued):

1 Donald Jewell, Assistant Director
Central Training Academy
US DOE/AL
PO Box 5400
Albuquerque, NM 87115

1 Ronald Perry
Argonne National Laboratory
Bldg. 222 Electronics
Argonne National Laboratory
9700 South Cass Avenue
Argonne, IL 60439

1 Roger L. Black
W. Patrick Keeney
Argonne National Laboratory
Bldg. 752/MS 6000
PO Box 2528
Idaho Falls, ID 83403

1 Larry Runge and George Schoener
Safeguards and Security Division
Bldg. 50
2400 Upton Road
Upton, NY 11973

1 Kris Dahms
Safeguards and Security Division
Bldg. 703
2400 Upton Road
Upton, NY 11973

1 Robert L. Windus, Security Officer
US DOE/BP
PO Box 3621
Portland, OR 87208

1 Harold W. Kelley, Director
Safeguards and Security Division
US DOE/CH
9800 South Cass Avenue
Argonne, IL 60439

1 Rudy Dorner
Fermi National Accelerator Laboratory
MS 102
Batavia, IL 60150

1 H. R. Martin, Acting Director
Safeguards and Security Division
US DOE/ID
785 DOE Place
Idaho, Falls, ID 83402

1 Timothy L. Mitchell, L 024
Lawrence Livermore National Laboratory
PO Box 808
Livermore, CA 94550

1 Darryl B. Smith
James W. Tape
N-DO/MS E550
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 Jack England, Division Leader
OS-DO, MS G729
Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

1 E. Wayne Adams, Director
Safeguards and Security Division
US DOE/NV
PO Box 98518
Las Vegas, NV 89193-8518

1 William G. Phelps, Director
Safeguards and Security Division
US DOE/OR
PO Box 2001
Oak Ridge, TN 37831-8570

1 J. A. Bullian, Director
Safeguards and Security Division
US DOE/PNR
PO Box 109
West Mifflin, PA 15122

2 Joseph W. Wiley, Director
Safeguards and Security Div
US DOE/RL
PO Box 550
Richland, WA 99352

DISTRIBUTION (Continued):

1 Michael Hooper, Acting Director
Safeguards and Security Division
US DOE/SF
Lawrence Livermore Laboratories
L-556
PO Box 808
Livermore, CA 94550

1 Gerorge G. Stefani, Jr., Director
Security and Safeguards Division
Schenectady Naval Reactors Office
US DOE
PO Box 1069
Schenectady, NY 12301

1 Donald J. Ornick, Director
Security Division
US DOE/OR
900 Commerce Road East
New Orleans, LA 70123

1 H. B. Gnann, Chief
Safeguards Engineering and Projects Branch
US DOE/SR
PO Box A
Aiken, SC 29808

1 Joan Christopher, Security Officer
Western Area Power Administration
US DOE
PO Box 3402
Golden, CO 80401

1 Larry Cameron
Allied Signal, Inc., Kansas City Division
2000 E. 95th Street
Kansas City, KS 64131-3095

1 Edward C. McGurren, Manager
Security Operations
Allied Signal, Inc., Kansas City Division
2000 E. 95th Street
Kansas City, KS 64131-3095

1 Harley Toy, Manager
Nuclear Services
Battelle Memorial Institute
505 King Avenue
Columbus, OH 43201

1 Boeing Petroleum Services
Attn: Security Department
850 South Clearview
New Orleans, LA 70123

1 John W. Jones, Manager
Safeguards and Security
EG&G Idaho
1955 Fremont
Idaho Falls, ID 83402-3126

1 Daniel Baker, Manager
Security
EG&G Mound
Bldg. 99
PO Box 3000
Miamisburg, OH 45432

1 K. N. Gardner
Technical Security
Bldg. 99
EG&G Mound
PO Box 3000
Miamisburg, OH 45432

1 Ron Mahan, Manager
Security Administration
EG&G Mound
Bldg. 99
PO Box 3000
Miamisburg, OH 45432

1 Vince Hanson, Manager
Protective Force
Bldg. 47
EG&G Mound
PO Box 3000
Miamisburg, OH 45342

1 Curtis L. Fellers
Technologies Department
Bldg. OSE-211
EG&G Mound
PO Box 3000
Miamisburg, OH 45342

DISTRIBUTION (Continued):

1 Roy E. Gmitter, Manager
Plant Security
General Electric Neutron Division
PO Box 2908
Largo, FL 34649

1 Holmes and Narver, Inc.
Attn: Electronics Department
PO Box 93838
Las Vegas, NV 89193-3838

1 Clifford A. Druit, Manager
Y-12 Safeguards and Security
Martin Marietta Energy Systems
Bldg. 9706-1, MS 8213
PO Box 2009
Oak Ridge, TN 37831-8213

1 James Hallihan
Mason and Hanger-Silas Mason, Co., Inc.
Pantex Plant
PO Box 30020
Amarillo, TX 79177

1 James Long
Protection Technologies of Idaho
785 DOE Place
Idaho Falls, ID 83402

1 Jeffrey Jay, Team Manager
Inspection and Technical Assessment Branch
Science Applications International Company
c/o DOE/Savannah River Operations Office
PO Box A
Aiken, SC 29802

1 Wackenhut Services, Inc.
800 West Commerce Rd., Suite 100
New Orleans, Louisiana 70123

1 Walk, Haydel, and Associates
600 Carondelet
New Orleans, LA 70130

1 Edward R. Saxon, Chief
Hanford Patrol
Westinghouse Hanford Company
SO-46
PO Box 1970
Richland, WA 99352

1 E. L. Goldman
Westinghouse Idaho Nuclear Company, Inc.
PO Box 4000
Idaho Falls, ID 83403

1 Ronald D. Klingler, Manager
Safeguards and Security
Westinghouser Idaho Nuclear Co., Inc.
MS 5102
PO Box 4000
Idaho Falls, ID 83403

1 Larry Schenk, Manager
Technical Security
Westinghouse Idaho Nuclear Company, Inc.
PO Box 4000
MS 5102
Idaho Falls, ID 83403

1 James M. Miller, Manager
Safeguards and Security
Westinghouse Materials Company of Ohio
PO Box 398704
Cincinnati, OH 45239

1 W. W. Arra
Westinghouse Savannah River Co., WSRS
703-57A, Rm. 7
PO Box 616
Aiken, SC 29802

1 M. Brinton
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 110
PO Box 616
Aiken, SC 29802

1 C. J. O. Cox
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 150
PO Box 616
Aiken, SC 29802

1 J. W. Maloney, Manager
Safeguards and Security
Westinghouse Savannah River Co., WSRS
PO Box 616
Aiken, SC 29802

DISTRIBUTION (Concluded):

1 S. C. Nashatker
Westinghouse Savannah River Co., WSRS
703-45A, Rm. 151
PO Box 616
Aiken, SC 29802

1 W. W. Rajczar
Westinghouse Savannah River Co., WSRS
703-42A, Rm. 115
PO Box 616
Aiken, SC 29802

1 John M. Samuels, Managers
Safeguards and Security Department
Westinghouse Savannah River Co., WSRS
PO Box 616
Aiken, SC 29802

1	3430	R. P. Kelly
1	3431	J. A. Kaiser
1	3432	D. E. Kerome
1	3433	R. M. Workhoven
1	3437	R. G. Baca
1	5200	J. Jacobs
1	5210	C. C. Hartwigsen
1	5211	S. H. Scott
1	5219	R. W. Moya
1	5220	J. W. Kane
1	5230	H. M. Witek
1	5231	D. J. Gangel
1	5233	D. C. Hanson
1	5234	J. C. Mitchell
1	5238	R. F. Davis
1	5240	D. S. Miyoshi
10	5240A	M. W. Green
1	5245	I. G. Waddoups
20	5245	J. P. Holmes
1	5245	L. S. Wright
1	5248	R. P. Syler
5	5248	R. L. Maxwell
1	5249	B. J. Steele
1	5260	J. R. Kelsey
1	5268	S. J. Weissman
1	8530	M. A. Pound
1	8531	D. R. Charlesworth
1	8536	C. L. Knapp
1	8523	R. C. Christman
5	3141	S. A. Landenberger
8	3145	Document Processing For DOE/OSTI
3	3151	G. C. Claycomb